New Cryptosystem Using The CRT And The Jordan Normal Form

Hemlata Nagesh[1] and Birendra Kumar Sharma[2]

School of Studies in Mathematics,Pt.Ravishankar Shukla University Raipur(C.G.).
E-mail:5Hemlata5@gmail.com[1]
School of Studies in Mathematics,Pt.Ravishankar Shukla University Raipur(C.G.).
E-mail:sharmabk07@gmail.com[2]

Abstract

In this paper we introduce a method for improving the implementation of GGH cryptosystem using the Chinese Remainder Theorem (CRT) and jordan normal form. In this paper we propose a method for improving the speed of Babai's Round- Off CVP approximation algorithm [1] in lattices using the Chinese Remainder Theorem (CRT) then formulate a new lattice-based cryptosystem usng jordan normal form instead of hermite normal form would improve substantially the efficiency of the lattice based cryptosystem having Goldreich-Goldwaser-Halevi cryptosystem.

Keywords: *Lattices; Jordan Normal Form;CRT.*
MSC No: 94A60

1 Introduction

The RSA public key cryptosystem [11] based on difficulty of factoring in to primes has made an important contribution in the field of asymmetric cryptography. In this direction, ElGamal cryptosytem [5] was the other public key system which was based on difficulty of discrete logarithm problem. Several extensions were made of these two systems improving efficiency and security.

Recent advancements in the field of lattice-based cryptography have brought a sustained interest in producing a lattice-based cryptosystem that runs in a similar space and time complexity as existing conventional asymmetric key cryptosystems. Two specific related cryptosystems showing much promise are the cryptosystems introduced by Goldreich, Goldwasser and Halevi [5] (GGH), and its modification and improvement by Micciancio [9].

Now, in this paper, we use Jordan normal form in such a way that for any lattice it will have small representation which improves the security of our

proposed scheme. The technique described in this paper can be used to significantly reduce the key size of GGH like cryptosystems mentioned in [10].and we propose a method for improving the speed of Babai's Round- Off CVP approximation algorithm [1] in lattices using the Chinese Remainder Theorem (CRT). We then formulate a new lattice-based cryptosystem usng jordan normal form instead of hermite normal form would improve substantially the efficiency of the lattice based cryptosystem having Goldreich-Goldwaser-Halevi cryptosystem.

In particular, our technique gives encryption schemes that are more secure and efficient than other GGH invariants .First, we recall some basic definitions and properties of lattices and describe new cryptosystem using CRT and Jordan normal form and analyzed the security and the space efficiency of the new cryptosystem.

2 Preliminaries

2.1 Lattice

Let B=$\{b_1, b_2, b_3.....\}$ be a set of n linearly independent vectors in $\mathbb{R}^m$ The lattice generated by B is the set $L\{B\}= \{\sum_i x_i b_i | x_i \epsilon \mathbb{Z}\}$ of all integer linear combinations of the vectors in B. The set B is called basis and it is usually identified with the matrix B=$[b_1,b_2,b_3.....b_n]$ $\epsilon \mathbb{R}^{m\times n}$ having the vectors.$b_i$as columns.

The matrix $L\{B\}$ is full rank if n=m,i.e. if B spans the entire vector space $\mathbb{R}^m$. over the reals for simplicity, in the rest of this paper we will consider only full rank lattices.

2.2 Jordan Normal Form

A Jordan normal form (often called Jordan canonical form) of a linear operator on a finite-dimensional vector space is an upper triangular matrix of a particular form called a Jordan matrix, representing the operator on some basis. The form is characterized by the condition that any non-diagonal entries that are non-zero must be equal to 1, be immediately above the main diagonal (on the superdiagonal), and have identical diagonal entries to the left and below them.

An $n \times n$ matrix A is diagonalizable if and only if the sum of the dimensions of the eigenspaces is n.there is an invertible matrix P such that $A = PJP^{-1}$, where The matrix J is almost diagonal This is the Jordan normal form of A. Every square matrix A can be put in Jordan normal form is equivalent to the

claim that there exists a basis consisting only of eigenvectors and generalized eigenvectors of A.

3 Chinese Remainder Theorem

Let $p_i \epsilon N$ n coprimes integers,$P = \Pi_{i=1}^{n} p_i$ and $P_i = P/p_i$ Then, for any n-tuple ai there exists an unique integer$0 \leq A < P$ such that $a_i = A mod p_i$,

$A = \sum_{i=1}^{n} a_i (P_i^{-1} mod p_i) P_i mod P$

4 The GGH Cryptosystem Using CRT and Jordan Normal Form

The Goldreich Goldwasser-Halevi (GGH) cryptosystem relies on the difficulty on the closet vector problem (CVP) in a lattice. The system is reminiscent of the McEliece cryptosystem encryption because both systems are randomized. The ciphertext in GGH encryption is considerably larger than the message. Hence, Miccinancio [10] proposed a variant of the GGH cryptosystem. The first chosen the public key to be the Hermite normal form of private key and the secondly to encode the message in the error vector rather than in the lattice point in order to reduce it to the orthogonalized parallelepiped. This resulted in to significantly shorter ciphertexts as compare to the original GGH system and makes the encryption process deterministic.

We design this new scheme specifically to provide faster operations, in a particular faster implementation, while still maintaining a similar structure to existing cryptosystems. Specifically, this involved consideration in the design for decryption using the CRT round-off method and jordan normal form.

4.1 Key Generation

4.1.1 Private Key

:

To create the private basis, we use GGH's private basis construction, namely $R \leftarrow bI + M$. This was chosen over Micciancio's basis construction for two reasons. Firstly, it allows us to make generalizations about the bound on the size of $\| R_\infty \|$ which allows for much faster key generation as we do not need to perform a full matrix inversion. Secondly, and perhaps more importantly, it provides a more orthogonal basis with which to perform decryption,

which in turn, decreases the size necessary to ensure correct decryption using CVP Round-off. This in turn allows us to decrease the size of the coefficients while keeping the same security parameter, saving storage and transmission space and increasing efficiency.

4.1.2 Public Key

:

To create the public basis, we use method of ap- plying a JNF on the private basis, as this provided a greater level of security, simplified key storage and much smaller public keys.

We are able to significantly speed up the decryption phase by precomputing all the required values of the functions $Q(p)$ and $R'(p)$ in the key generation phase and storing these values in a look-up table. This increases the speed of the decryption step, at the expense of a lower key generation speed.

5 Algorithm

5.1 Input

$n \epsilon N$ the security parameter.

5.2 Output

$B \epsilon Z^n$ the public key,
$R \epsilon Z^{n,n}$ the private key.
begin
$M \leftarrow$ 0for i; j 0 to n-1 do
$M_{i,j} \leftarrow Rand(-1, 1)$
$b \leftarrow \lceil 2\sqrt{2n/3} \rceil$ repeat $b \leftarrow b + 1$ until $\| (bI + M)^{-1} \|_\infty \leq 1/2$
$R \leftarrow bI + M$
$B = JNF(R)$
end

5.3 Encryption Process

: We now describe how Alice wraps and sends a message to Bob using the public key.For encryption, we use Micciancio's method of modulo lattice reduction with the public basis. We felt that this provided excellent speed and provided strong notions of security. We modified Micciancio's construction by limiting the encryption vector domain to -1, 0, 1 and by using
$\| R^{-1} \| < 1/2$.

5.4 Decryption Process

Decryption is of a similar form to the improved GGH decryption method using CRT except with a minor change to re ect the encoded message being in the error vector rather than the lattice point. i.e. given the lattice vector w, we calculate the plaintext $p = c - w$

6 Security Considerations

We now discuss the security of the new GGH Cryptosystem using jordan normal form and CRT under passive attacks.

1.Try to obtain private key B from the public key B'.

2.Try to obtain information about the message from the cipher text,given that the error vector is small.

6.1 Computing a Private Key

For the first attack, we simply run a lattice basis reduction algorithm on the public basis B'.If we are lucky then it will output a basis B" that is good enough to allow the efficient solution of the required closest vector instances.

To prevent such an attack it is necessary that the dimension of the lattice be sufficiently large.

6.2 Computation Information About The Message

To defeat this attack one use some not naively encode the message as a vector m$\epsilon\mathbb{Z}^n$,instead one should only use some low order bits of some entries of m to carry information or use an appropriate randomised padding scheme.

7 Memory usage

Since each finite field is independent, it is possible to decrypt a plaintext via CRT serially with respect to the key, i.e., only loading each matrix over some finite field into memory as we require it. This has great benefits for memory utilization especially for embedded systems as we are only required to store a matrix of standard integers in primary memory at any given time rather than a matrix of much larger variable-precision integers. In the case of lattice dimension 1000, it can be seen that the memory usage would only be approximately 4Mb at any given time. Obviously in such a case, decryption speeds would be I/O bound in the case of loading each matrix in from a hard drive or ash-based storage.

8 Conclusion

We have presented a new cryptosystem using CRT and Jordan normal form. The new cryptosystem is shown as secure as old one. Because the security of the new function reduces both the time and space requirements.We apply the Chinese Remainder Theorem to lattice-based cryptosystems by operating the cryptosystem in an integer ring with an order greater than the largest element,since working with variable precision integers larger than the implementation machine's word-size imposes a significant overhead.and the use of jordan normal form shows that the number of lattices in a certain dimension is exponential in its bit size representation of their Jordan normal form and thus the JNF representation is essentially optimal if one considers arbitrary lattices. The improved efficiency allows even bigger value of the security parameter while maintaining the scheme reasonably practical.

References

[1] M.Ajtai. Generating hard instances of lattice problems (extended abstract). In Proceeding of the twenty eighth Annual ACM Symposium on the theory of Computing (22-24 May 1996).Pg.

99- 108.Philadelphia,Pennsyvania

[2] M.Ajtai and C.Dwork. A public key cryptosystem with worst case/average case equivalance. In Procedding of the twenty eighth Annual ACM Symposium on the theory of Computing (4-6 May1997) Pg.284-293,El Paso,Texas, 6 IMPROVING LATTICE BASED USING THE CRYPTOSYSTEM JORDAN NORMAL FORM

[3] L.Babai. On Lovasz lattice reduction and the nearest lattice point problem. Combinatirica.6(1) (1986) Pg.1-13

[4] J.Y.Cai and T.W.Cusick. A lattice based public key cryptosystem.Information and Computation,151(1-2) (May -June 1999).Pg.17-31

[5] Taher ElGamal .A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory 31 (4) (1985). Pg.469-472

[6] R.Fischlin and J.P.Seifert.Tensor basedtrapdoors for CVP and their application to public key cryptography.In 7th IMAInternational Conference"Cryptography and Coding",volume 1746 of Lecture Notes in Computer Science,pages (1999) Pg. 244-257,Springer-Verlag .

[7] O.Goldreich,S.Goldwasser, and S.Halevi.Public key cryptosystems from lattice reduction problems. In B.S.Kaliski Jr.editor Advance in cryptology-CRYPTO'97 volume 1294 of lecture notes in Computer Science.pages (Aug1997).Pg.112-131.Springer Verlag.17-21

[8] J.Hoffstein ,J.Pipher, and J.H.Silverman.NTRU:A ring based public key cryptosystem.In J.Buhler,editor,Algorithmic Number Theory(ANTS III) volume 1423 of lecture Notes in Computer Science,(1998) Pg. 267-288.Portland,OR, ,Springer

[9] R.J.McEliece.A public key cryptosystem based on algebraic coding theory,DSN Progress report (1978) Pg.42-44.Jet Propulsion Laboratory,Pasadena

[10] D. Micciancio, Improving lattice based cryptosystems using the Hermite normal form, Cryptography and Lattices (CaLC) (J. H. Silverman, ed.), LNCS, vol. 2146(Springer, 2001) Pg.126-145

[11] R.Rivest, A. Shamir, L. Adleman (1978).A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.Communications of the ACM 21 (2),(1978) Pg .120126.